2000

The proof of Fermat's last theorem

Mohamad Trad

Follow this and additional works at: https://scholarworks.lib.csusb.edu/etd-project

Part of the Number Theory Commons

Recommended Citation


This Project is brought to you for free and open access by the John M. Pfau Library at CSUSB ScholarWorks. It has been accepted for inclusion in Theses Digitization Project by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.
THE PROOF OF FERMAT'S LAST THEOREM

A Project
Presented to the
Faculty of
California State University,
San Bernardino

By
Mohamad Trad
December 2000

Approved by:

Jim Okon, Committee Chair,

Terry Hallett, Committee Member

John Sarli, Committee Member

Terry Hallett, Committee Member
Department Coordinator
Department of Mathematics

Charles Stanton, Chair
Department of Mathematics
Today we think of Fermat as perhaps the most famous number theorist who ever lived. Because Fermat refused to publish his work, his son, Samuel undertook the task of publishing his father’s mathematical ideas. Fermat’s Last Theorem states that the equation $x^n + y^n = z^n$ has no non-zero integer solutions for $x$, $y$ and $z$ when $n > 2$. We divided our project into four Chapters. In the first Chapter we introduce the Legendre Symbol and some properties of this symbol. We also through the Legendre Symbol define quadratic residues and nonresidues. We give a proof of Gauss’s Lemma and the Quadratic Reciprocity Theorem. In Chapter Two, we introduce the ring $\mathbb{Z}[w]$. We first define the ring and give some properties of $\mathbb{Z}[w]$. Next we prove the division algorithm and a unique factorization theorem in $\mathbb{Z}[w]$. Later in the Chapter we find the units and primes in $\mathbb{Z}[w]$. At last we show that prime and irreducible numbers are equivalent in $\mathbb{Z}[w]$. In Chapter Three, we give Fermat’s only known proof of his theorem in the case when $n = 4$ using primitive Pythagorean triples. Before the proof of the case $n = 3$ of Fermat’s Last Theorem, which was attributed to Euler, we define the order of an element of $\mathbb{Z}[w]$. We also give a proof of some Lemmas that were important for the proof of this case of Fermat’s Last Theorem as well as the proof of Sophie
Germain's Theorem. For example we prove that if \( x \) and \( y \in \mathbb{Z}[w] \) are not associates then \( \text{ord}(xy) = \text{ord}(x) + \text{ord}(y) \). In the proof we use the division algorithm in \( \mathbb{Z}[w] \), norm and order notation, and the unique factorization theorem. The proof of the case \( n = 3 \) is given next and depends on several properties of \( \mathbb{Z}[w] \) developed in Chapter Two. The proof of the case \( n = 3 \) was originally given by Euler in 1753. Next we give a proof of Sophie Germain's Theorem, which splits Fermat's Last Theorem into two cases. Case 1 when none of \( x, y \) and \( z \) are divisible by \( n \) and case 2 when one and only one of \( x, y, z \) is divisible by \( n \). In the last Chapter, we mention some recent results related to Fermat's Last Theorem. The most important result is the famous conjecture of Shimura-Taniyama which led to the proof of Fermat's Last Theorem by Andrew Wiles in 1994.
ACKNOWLEDGMENTS

I will first address my gratitude and thanks to my advisor and leader, making my mission possible, Dr. James Okon. I acknowledge the time and effort that he spent with me for three quarters doing his best to help me accomplish my dream, which came true with his help. I would like also to thank Dr Okon for understanding my questions and my problems and for making my mission fruitful and educationally helpful. I would like to thank the mathematics department from dean to secretary to teachers for their help and support during my master degree. I would like to thank my parents and brother for their emotion and financial support. I would like finally to thank God for his blessing.
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>v</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER 1</td>
<td>4</td>
</tr>
<tr>
<td>CHAPTER 2</td>
<td>14</td>
</tr>
<tr>
<td>CHAPTER 3</td>
<td>24</td>
</tr>
<tr>
<td>CHAPTER 4</td>
<td>39</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>44</td>
</tr>
</tbody>
</table>
INTRODUCTION

When Pierre de Fermat died in 1665 he was one of the most famous mathematicians in Europe. Today Fermat’s name is almost synonymous with number theory. There are two surprising facts about Fermat’s fame as a mathematician. The first is that he was not a mathematician at all, but a jurist. Throughout his mature life he held rather important judicial positions in Toulouse, and his mathematical work was done as an avocation. The second is that he never published a single mathematical work. Fermat was very jealous, secretive and competitive about his work. His son, Samuel, undertook the task of publishing.

Samuel, in the margin of the copy of Diophantus found the statement of the theorem. This simple statement, which can be written in symbols as “for any integer \( n > 2 \) the equation, \( x^n + y^n = z^n \), is impossible” is known as Fermat’s Last Theorem. It is very possible the name came from the fact that this theorem was his last theorem. The edition of Diophantus, which Fermat used, was the edition of Bachet (1581-1638). It was a translation of Diophantus work from the original Greek into Latin with some added comments. Fermat was pursuing a line of investigation that was initiated by Bachet who was inspired by Diophantus. This investigation led Fermat to the proof of the case \( n = 4 \).
Since the Arithmetic of Diophantus deals exclusively with rational numbers, it goes without saying that Fermat meant that there are no rational numbers \( x, y, z \) such that 
\[ x^n + y^n = z^n \quad (n > 2) \]. Fermat's Last Theorem amounted essentially to saying that if \( n \) is an integer greater than 2 then it is impossible to find positive whole numbers \( x, y, z \) such that 
\[ x^n + y^n = z^n \]. This is the form in which the theorem is usually stated.

In this project, we divided our work into four Chapters. The first Chapter deals with the law of Quadratic Reciprocity which characterizes the solutions to the equation 
\[ x^2 \equiv n \pmod{p} \] where \( p \) is an odd prime. We prove Gauss's Lemma which says that \( x^2 \equiv n \pmod{p} \) has a solution if the sequence \( a, 2a, ..., \frac{(p-1)}{2}a \) has an even number of negative least residues. We conclude this Chapter with the proof of law of Quadratic Reciprocity and some examples of its application to determine whether or not a number is a quadratic reciprocal. Early attempts to solve Fermat's Last Theorem led to the question of what arithmetic properties of \( \mathbb{Z} \) carry over to sub-rings of the field of complex numbers. In the third Chapter, we give several proofs of special cases of Fermat's Last Theorem. We first give the proof in the case \( n=4 \). This is the only case known to be proven by
Fermat. The case $n=3$ was proven around 1753 by Euler. The last case is Sophie Germain's Theorem. In the last Chapter, Chapter Four, we give a summary of the history of Fermat's Last Theorem. We include a brief overview of some recent results that led to the proof of Fermat's Last Theorem.
CHAPTER ONE

We first define the Legendre symbol.

Definition 1.1 Let \( p \) be a prime and let \( a \) be an integer. Then we define the Legendre symbol, \( \left( \frac{a}{p} \right) \), to be 0 if \( p \mid a \). Now if \( p \) does not divide \( a \) then we define \( \left( \frac{a}{p} \right) \) as follows:

\[
\left( \frac{a}{p} \right) = 1 \quad \text{if } x^2 \equiv a \pmod{p} \text{ has a solution, that is if } a \text{ is a quadratic residue.}
\]
\[
\left( \frac{a}{p} \right) = -1 \quad \text{if } x^2 \equiv a \pmod{p} \text{ has no solution, that is if } a \text{ is a quadratic nonresidue.}
\]

Example 1.1 If \( p = 7 \) then the quadratic residues (mod 7) are the least positive residues (mod 7) of \( 1^2, 2^2, \) and \( 3^2 \), namely, 1, 4, and 2. The quadratic nonresidues (mod 7) are 3, 5, and 6. Thus \( \left( \frac{1}{7} \right) = \left( \frac{2}{7} \right) = \left( \frac{4}{7} \right) = 1 \) and \( \left( \frac{3}{7} \right) = \left( \frac{5}{7} \right) = \left( \frac{6}{7} \right) = -1 \).

Definition 1.2 If \( \gcd(a,n) = 1 \) and \( a \) is of order \( \phi(n) \) modulo \( n \), then \( a \) is a primitive root of the integer \( n \).

Next we will prove some properties about the Legendre symbol.

Proposition 1.1 Let \( p \) be an odd prime with \( \gcd(a,p) = 1 \). Then \( a \) is a quadratic residue of \( p \) if and only if

\[
\left( \frac{a}{p} \right) = \left( \frac{a^{(p-1)/2}}{p} \right) = 1 \pmod{p}.
\]
Proof. Suppose that $a$ is a quadratic residue of $p$, so that $x^2 \equiv a \pmod{p}$ has a solution, call it $x_1$. Since $\gcd(a, p) = 1$, then $\gcd(x_1, p) = 1$. By Fermat's Theorem

$$a^{\frac{(p-1)}{2}} \equiv (x_1^{\frac{(p-1)}{2}})^2 \equiv x_1^{p-1} \equiv 1 \pmod{p}.$$  

For the opposite direction, assume that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, and let $r$ be a primitive root of $p$. Then $a \equiv r^k \pmod{p}$ for some integer $k$, with $1 \leq k \leq p-1$. It follows that

$$r^{\frac{k(p-1)}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$  

From group theory the order of $r$, which is $p-1$, must divide the exponent $\frac{k(p-1)}{2}$. We conclude that $k$ must be even, $k = 2j$. Hence, $(r^j)^2 = r^{2j} = r^k \equiv a \pmod{p}$. Then the integer $r^j$ is a solution of $x^2 \equiv a \pmod{p}$. Now $a$ is a quadratic residue of the prime $p$. □

Corollary 1.1 Let $a, p$ be integers with $p$ a prime then

$$a^\frac{p-1}{2} \equiv (-a)^{\frac{p-1}{2}} \pmod{p}.$$  

Proof. If $p$ is an odd prime and $\gcd(a, p) = 1$ then by Fermat's Theorem the following congruence is true:

$$(a^\frac{p-1}{2} - 1)(a^\frac{p-1}{2} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p}.$$  

Hence either $a^\frac{p-1}{2} \equiv 1 \pmod{p}$ or $a^\frac{p-1}{2} \equiv -1 \pmod{p}$ but not both. By Proposition 1.1, $a$ is a quadratic residue of the prime $p$. □
quadratic residue if and only if \( a - \equiv l (\text{mod} \ p) \). Hence

\[ a^2 \equiv -l (\text{mod} \ p) \]

if and only if \( a \) is a quadratic non-residue.

In conclusion, the following congruence is true:

\[ a^2 \equiv (\frac{a}{p}) (\text{mod} \ p) \].

Proposition 1.2 Let \( a \), \( b \) and \( p \) be integers with \( p \) a prime. Then each of the following is true:

a) \( \left( \frac{ab}{p} \right) \equiv \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) (\text{mod} \ p) \).

b) If \( a \equiv b (\text{mod} \ p) \) then \( \left( \frac{a}{p} \right) \equiv \left( \frac{b}{p} \right) \).

c) If \( p \) does not divide \( a \) then \( \left( \frac{a}{p} \right) \left( \frac{-a}{p} \right) = 1 \).

Proof. a) We have \( \left( \frac{ab}{p} \right) \equiv (ab)^{p-1} \equiv a^{p-1} b^{p-1} \equiv \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) (\text{mod} \ p) \).

b) If \( a \equiv b (\text{mod} \ p) \), then \( x^2 \equiv a (\text{mod} \ p) \) and \( x^2 \equiv b (\text{mod} \ p) \) have the same number of solutions. Thus \( x^2 \equiv a (\text{mod} \ p) \) and \( x^2 \equiv b (\text{mod} \ p) \) are both solvable or neither one has a solution.

In conclusion, the following equality is true: \( \left( \frac{a}{p} \right) = \left( \frac{b}{p} \right) \).

From part (a), \( \left( \frac{a}{p} \right) \left( \frac{-a}{p} \right) = \left( \frac{a^2}{p} \right) \). Since \( x^2 \equiv a^2 (\text{mod} \ p) \) has a solution, \( \left( \frac{a^2}{p} \right) = 1 \).
Definition 1.3 The set \( \{-\frac{p-1}{2}, \ldots, 0, \ldots, \frac{p-1}{2}\} \) is called the set of least residues mod \( p \). If \( p \) does not divide \( a \) then \( M(a) \) is the number of negative least residues in the set \( \{a, 2a, \ldots, \frac{(p-1)a}{2}\} \).

Most proofs of the Quadratic Reciprocity Law rest ultimately upon what is known Gauss' Lemma.

Gauss Lemma. If \( p \) is an odd prime and \( \gcd(a,p)=1 \) then \( \left(\frac{a}{p}\right) = (-1)^{M(a)} \).

Proof. Let \( m_i \) be the least residue of \( ta \) and \( -m_i \) be the least residue of \( t' \) for \( 1 \leq t, t' \leq \frac{p-1}{2} \). Suppose we have \( m_i \equiv ta (\text{mod } p) \) and \( -m_i \equiv t'a (\text{mod } p) \) for some \( t, t' \) such that \( 1 \leq t, t' \leq \frac{p-1}{2} \). Since \( \gcd(a,p) = 1 \) and \( a(t+t') \equiv 0 (\text{mod } p) \) then \( (t+t') \equiv 0 (\text{mod } p) \) which is impossible since \( 2 \leq t+t' \leq p-1 \).

Similarly if \( m_i \equiv ta \equiv t'a (\text{mod } p) \) then \( (t-t')a \equiv 0 (\text{mod } p) \). Since \( \gcd(a,p) = 1 \), \( (t-t') \equiv 0 (\text{mod } p) \) which is impossible. We can now conclude that all \( \pm m_i \) are distinct and none is zero. Now \( ta \equiv \pm m_i (\text{mod } p) \) and \( m_i \neq m_k \) for \( t \neq k \). Therefore \( \prod_{k=1}^{\frac{p-1}{2}} \pm m_i = \prod_{k=1}^{\frac{p-1}{2}} ka \). Now
Therefore \((-1)^{M(a)} \frac{p-1}{2}! \equiv a^\frac{p-1}{2} (\frac{p-1}{2})! \pmod{p}\). Since \(\frac{p-1}{2}\) is relatively prime to \(p\), \((-1)^{M(a)} \equiv a^\frac{p-1}{2}\pmod{p}\). By Corollary 1.1 of Proposition 1.1, we have \(\frac{a}{p} \equiv a^\frac{p-1}{2} \equiv (-1)^{M(a)} \pmod{p}\). □

Example 1.2 We will evaluate \(\left(\frac{3}{11}\right)\). The least residues of 3, 6, 9, 12, 15 are 3, -5, -2, 1, 4\pmod{11}\). We conclude that

\(\left(\frac{3}{11}\right) = (-1)^2 = 1\). Indeed 3 \(\equiv 5^2 \pmod{11}\).

Next we consider \(\left(\frac{7}{13}\right)\). The least residues of 7, 14, 21, 28, 35, 42 are -6, 1, -5, 2, -4, 3\pmod{13}\). Then \(\left(\frac{7}{13}\right) = (-1)^3 = -1\) and 7 is a quadratic non-residue of 13.

Lemma 1.1 If the integer \(n\) is an odd positive integer then for all complex numbers \(x\) and \(y\) we have

\[x^n - y^n = \prod_{k=0}^{n-1} (\xi^k x - \xi^{-k} y) \text{ where } \xi = e^{\frac{2\pi i}{n}}.\]
Proof. We can factor \( z^n - 1 \) as \( z^n - 1 = \prod_{k=0}^{n-1} (z - \zeta^k) \). Now if 

\[
    z = \frac{x}{y} \quad \text{then} \quad \frac{x^n - y^n}{y^n} = \prod_{k=0}^{n-1} \left( 1 - \frac{y}{y} \zeta^k \right) \quad \text{and} \quad x^n - y^n = \prod_{k=0}^{n-1} (x - y \zeta^k). 
\]

Since \( \{ \zeta^k \}_{k=0}^{n-1} \) is a group of order \( n \), then 

\[
    \text{ord}(\zeta^{-2}) = \text{ord}(\zeta^{n-2}) = \frac{n}{\gcd(n, n-2)} = n. 
\]

Therefore we have 

\[
    \{ \zeta^{-2k} \}_{k=0}^{n-1} = \{ \zeta^k \}_{k=0}^{n-1}. 
\]

Now 

\[
    x^n - y^n = \prod_{k=0}^{n-1} (x - y \zeta^k) = \prod_{k=0}^{n-1} (x - y \zeta^{-2k}) = \prod_{k=0}^{n-1} \zeta^{-k} (x \zeta^k - y \zeta^{-k}). 
\]

By factoring out \( \zeta^{-(1+2+\ldots+(n-1))} = 1 \), we get the requested result 

\[
    x^n - y^n = \prod_{k=0}^{n-1} (x \zeta^k - y \zeta^{-k}). 
\]

\[
\]

The following two propositions are technical results used in the proof of the Quadratic Reciprocity Theorem.

Proposition 1.3 If \( n \) is an odd positive integer and 

\[
    f(z) = e^{2\pi i z} - e^{-2\pi i z} \quad \text{then} \quad \frac{f(nz)}{f(z)} = \prod_{k=1}^{n-1} f(z + \frac{k}{n}) f(z - \frac{k}{n}). 
\]

Proof. Let \( x = e^{2\pi i z} \) and \( y = e^{-2\pi i z} \). By using the previous Lemma, 

\[
    f(nz) = \prod_{k=0}^{n-1} \left( e^{\frac{2\pi ik}{n}} - e^{-\frac{2\pi ik}{n}} \right) = \prod_{k=0}^{n-1} \left( e^{2\pi i (z + \frac{k}{n})} - e^{-2\pi i (z + \frac{k}{n})} \right) = \prod_{k=0}^{n-1} f(z + \frac{k}{n}). 
\]
\[ f(nz) = f(z) \prod_{k=1}^{n-1} f\left(z + \frac{k}{n}\right) \]. Now \( f\left(z + \frac{k}{n} - 1\right) = e^{\frac{2\pi i (z + \frac{k}{n} - 1)}{n}} = e^{-\frac{2\pi i (z + \frac{k}{n} - 1)}{n}} \) so
\[ f\left(z + \frac{k}{n} - 1\right) = e^{\frac{2\pi i (z + \frac{k}{n})}{n}} - e^{\frac{-2\pi i (z + \frac{k}{n})}{n}} e^{2\pi i} \text{ and } e^{-2\pi i} = 1 = e^{2\pi i}. \] We can conclude that \( f(z - \frac{n-k}{n}) = f(z + \frac{k}{n} - 1) = f(z + \frac{k}{n}) \). So
\[ \frac{f(nz)}{f(z)} = \prod_{k=1}^{n-1} f\left(z + \frac{k}{n}\right) = \prod_{k=1}^{n-1} f\left(z + \frac{k}{n}\right) = \prod_{k=1}^{n-1} f\left(z - \frac{k}{n}\right) \]. Let \( k' = n - k \) then
\[ \frac{n+1}{2} \leq k \leq n-1 \] so \( 1 - n \leq -k \leq -\frac{n+1}{2} \) and \( 1 \leq n-k \leq \frac{n-1}{2} \). Then
\[ \frac{f(nz)}{f(z)} = \prod_{k=1}^{n-1} f\left(z + \frac{k}{n}\right) \prod_{k=1}^{n-1} f\left(z + \frac{-k}{n}\right) \text{ so } \frac{f(nz)}{f(z)} = \prod_{k=1}^{n-1} f\left(z + \frac{k}{n}\right)f\left(z + \frac{k}{n}\right). \]

**Proposition 1.4** If \( p \) is an odd prime and \( a \in \mathbb{Z} \), where \( p \) does not divide \( a \), then the following equality is true:
\[ \prod_{r=1}^{p-1} f\left(\frac{ta}{p}\right) = \left(\frac{a}{p}\right) \prod_{r=1}^{p-1} f\left(\frac{t}{p}\right). \]

Proof. Let \( ta \equiv \pm m_i (\text{mod} \, p) \) as in the proof of Gauss’s Lemma. Then \( ta = \pm m_i + \alpha_i \) where \( \alpha_i \in \mathbb{Z} \). So \( \frac{ta}{p} - \frac{\pm m_i}{p} = \alpha_i \in \mathbb{Z} \). Now by the definition of \( f(z) \) we can easily conclude that
\[ f\left(\frac{ta}{p}\right) = f\left(\frac{\pm m_i}{p}\right) = \pm f\left(\frac{m_i}{p}\right). \] By Gauss’s Lemma and since \( p \) is an odd prime we conclude:
We are now ready to prove the Law of Quadratic Reciprocity.

Theorem 1.1 (Law of Quadratic Reciprocity). Let $p, q$ be odd primes. Then \( \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \).

Proof. By the preceding Proposition we can conclude

\[
\prod_{t=1}^{p-1} f(t) = \prod_{t=1}^{q-1} f(t) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \prod_{t=1}^{\infty} f(t).
\]

Now solve for \( \left( \frac{q}{p} \right) \) to get

\[
\left( \frac{q}{p} \right) = \prod_{t=1}^{p-1} f\left( \frac{t}{p} \right) f\left( \frac{t-m}{p} \right).
\]

Similarly, since

\[
\left( \frac{p}{q} \right) = \prod_{t=1}^{q-1} f\left( \frac{t}{q} \right) f\left( \frac{t-m}{q} \right)
\]

then

\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = \prod_{m=1}^{p-1} \prod_{t=1}^{q-1} f\left( \frac{t}{p} \right) f\left( \frac{t}{q} \right) f\left( \frac{t-m}{p} \right) f\left( \frac{t-m}{q} \right).
\]
In conclusion, \( \frac{p}{q} = (-1)^{\frac{p-1}{2}} \frac{q}{p} \) by multiplying both sides by \( \frac{q}{p} \) we will get the requested result

\[
\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}} \frac{q}{p}.
\]

Note that Gauss' Lemma applies only to odd primes. In the case when \( q = 2 \) we have \( \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \) (Burton p: 187).

We conclude this Chapter with some examples.

Example 1.3 Consider the congruence \( x^2 \equiv -42 (\text{mod} 61) \). We have \( \left(\frac{-42}{61}\right) = \left(\frac{-1}{61}\right) \left(\frac{2}{61}\right) \left(\frac{3}{61}\right) \left(\frac{7}{61}\right) \) from part (a) of Proposition 1.2

and \( \left(\frac{2}{61}\right) = (-1)^2 = 1, \left(\frac{3}{61}\right) = (-1)^{\frac{61-1}{8}} = -1. \) By using the Law of Quadratic Reciprocity we have, \( \left(\frac{3}{61}\right) = \left(\frac{61}{3}\right) \left(\frac{2}{3}\right) \left(\frac{60}{2}\right) = \left(\frac{1}{3}\right) = 1 \) and

\[
\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right) \left(\frac{60}{7}\right) = \left(\frac{5}{7}\right) \left(\frac{4}{7}\right) = \left(\frac{5}{7}\right) \left(\frac{2}{7}\right) = \left(\frac{5}{7}\right) = (-1)^{\frac{24}{8}} = -1.
\]

Hence \( \left(\frac{-42}{61}\right) = 1 \) and \( x^2 \equiv -42 (\text{mod} 61) \) has a solution.
Example 1.4 Consider the congruence \( x^2 \equiv 3 \pmod{13} \). We have

\[
\left( \frac{3}{13} \right) = \left( \frac{13}{3} \right) \left( \frac{13-1}{2} \right) \left( \frac{3-1}{2} \right) = \left( \frac{1}{3} \right) = 1
\]

So \( x^2 \equiv 3 \pmod{13} \) has a solution.
CHAPTER TWO

Definition 2.1 The ring \( \mathbb{Z}[w] \) is the set of all expressions of the form \( a + wb \) where \( a, b \in \mathbb{Z} \).

Definition 2.2 Let \( \alpha \in \mathbb{Z}[w] \), \( \alpha \) is irreducible in \( \mathbb{Z}[w] \) if \( \alpha = ua \) implies \( u \) is a unit or \( a \) is a unit where \( u \) and \( a \in \mathbb{Z}[w] \).

Definition 2.3 Let \( a, b, p \in \mathbb{Z}[w] \). Then \( p \) is a prime in \( \mathbb{Z}[w] \) if \( p|ab \) then \( p|a \) or \( p|b \).

Definition 2.4 Let \( u \in \mathbb{Z}[w] \). If there exist a \( v \in \mathbb{Z}[w] \), such that \( uv=1 \), then \( u \) is a unit.

The following are some properties of \( \mathbb{Z}[w] \).

Lemma 2.1 Prove the following properties of the integral domain \( \mathbb{Z}[w] \) where \( w = \frac{-1}{2} + \frac{i\sqrt{3}}{2} \).

1) For \( w \in \mathbb{Z}[w] \) we have \( w^2 + w + 1 = 0 \) and \( w^3 = 1 \).

2) If \( \alpha \in \mathbb{Z}[w] \) then \( \alpha \) can written uniquely in the form \( a + wb \), where \( a, b \in \mathbb{Z}[w] \). Further, the conjugate of \( \alpha \), \( \overline{\alpha} = a - wb \) and \( N(\alpha) = a^2 - ab + b^2 \), where \( N(\alpha) \) is the norm of \( \alpha \).

Proof. 1) Since \( w \) is a primitive cube root of unity, \( w^2 + w + 1 = 0 \) and \( w^3 = 1 \).

2) Next assume \( \alpha = a + wb = a' + wb' \) where \( a, a', b, b' \in \mathbb{Z}[w] \). Then \( (a-a') + w(b-b') = 0 \). We conclude that \( a = a' \) and \( b = b' \). Next we
know that \( w^2 = -w - 1 \) and \( \bar{\alpha} = a + w^2 b = a + (-w - 1)b = a - b - wb \).

Finally,

\[
N(\alpha) = \alpha \bar{\alpha} = (a + wb)(a + w^2 b) = a^2 - ab + b^2.
\]

Definition 2.5 Let \( a, b, d \in \mathbb{Z}[w] \) with \( a, b \) are not both zero. We call \( d \) a greatest common divisor of \( (a, b) \) if \( d \mid a \), \( d \mid b \) and if \( c \mid a \) and \( c \mid b \), \( c \in \mathbb{Z} \), then \( c \mid d \). Note that if \( d, d' \) are greatest common divisors of \( (a, b) \) then \( d = ud' \) where \( u \) is a unit. If \( d \) is a gcd\((a, b)\) then we write \( d \in \text{gcd}(a, b) \). If \( 1 \in \text{gcd}(a, b) \) then we write \( \text{gcd}(a, b) = 1 \).

Lemma 2.2 is an important result about the norm of the product of two numbers in \( \mathbb{Z}[w] \).

Lemma 2.2 Let \( a, b \in \mathbb{Z}[w] \) then \( N(ab) = N(a)N(b) \).

Proof. Let \( a = x + wy \) and \( b = x' + wy' \) then

\[
N(ab) = (ab)(\bar{ab}) = (aa)(bb) = N(a)N(b). \]

The following proposition shows the Division Algorithm works in \( \mathbb{Z}[w] \).

Proposition 2.1 (Division Algorithm). The ring \( \mathbb{Z}[w] \) has a Division Algorithm. If \( \alpha, \beta \in \mathbb{Z}[w] \) and \( \beta \neq 0 \) then there exist \( \gamma, \delta \in \mathbb{Z}[w] \) satisfying \( \alpha = \beta \gamma + \delta \) and \( N\delta < N\beta \).

Proof. Let \( \frac{\alpha}{\beta} = r + os \) where \( s, r \) are rational numbers and...
choose $x, y$ to be integers satisfying $|r-x| \leq 1/2$ and $|s-y| \leq 1/2$.

Let $\gamma = x + yw$. Then \( \frac{\alpha}{\beta} - \gamma = (r-x) + (s-y)w \) and

\[
N\left(\frac{\alpha}{\beta} - \gamma\right) = (r-x)^2 + (s-y)^2 - (r-x)(s-y).
\]

Further, we have $(r-x)^2 \leq \frac{1}{4}$,

\[
(s-y)^2 \leq \frac{1}{4}, \quad -\frac{1}{2} \leq (r-x) \leq \frac{1}{2}, \quad \text{and} \quad \frac{1}{2} \leq (s-y) \leq \frac{1}{2}.
\]

As a result, $-\frac{1}{4} \leq (r-x)(s-y) \leq \frac{1}{4}$. Now, we can conclude

that $N\left(\frac{\alpha}{\beta} - \gamma\right) \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}$. Now let $\delta = \alpha - \beta \gamma$. Then

\[
N(\delta) = N(\beta)N\left(\frac{\alpha}{\beta} - \gamma\right) < N(\beta) \cdot 1 = N(\beta). \quad \text{Therefore} \quad \alpha = \beta \gamma + \delta \quad \text{with}
\]

$N(\delta) < N(\beta)$. □

In the following example, we will show that $\gamma$ and $\delta$ are not necessarily unique.

**Example 2.1** Divide $3+w$ by $2+w$ we get

$3+w = (1-w)(2+w)+w$ and $N(2+w) = 3 > 1 = N(w)$. Also

$3+w = 1(2+w)+1$.

**Lemma 2.3** Every pair of non-zero elements $a, b \in \mathbb{Z}[w]$ has a gcd. Further if $d \in \gcd(a,b)$ then $d = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}[w]$.

**Proof.** Let $a, b \in \mathbb{Z}[w]$ and let

$S = \{au+bv \text{ such that } N(au+bv) > 0\}$. The set $S$ is a non empty set
since \( a+b\in S \). Thus, by the well-ordering principle \( S \) must have an element with smallest norm \( d=au+bv \). If \( d \) does not divide \( a \) then \( a=qd+r, \) where \( 0<N(r)<N(d) \). By solving for \( r \), \( r=a-qd=a-(au+bv)d=(1-u)a+(-dv)b \) which is a contradiction since \( N(r)<N(d) \). Therefore \( d\mid a \) and, similarly, \( d\mid b \). If we have another number \( c \) such that \( c\mid a \) and \( c\mid b \) then \( c\mid d \) since \( d=au+bv \). Therefore \( d \) is a \( \text{gcd}(a,b) \). \( \Box \)

Note that we can have irreducible numbers which are not prime. For example, in \( \mathbb{Z}[[\sqrt{-5}]] \), \( 9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5}) \). If \( 3\mid (2+\sqrt{-5}) \) then \( 2+\sqrt{-5}=3(a+b\sqrt{-5}) \) so \( 3a=2 \) which is impossible. So \( 3 \) does not divide \( (2+\sqrt{-5}) \). Similarly, \( 3 \) will not divide \( (2-\sqrt{-5}) \). So \( 3 \) is not a prime. Now assume that \( 3=\alpha\beta \) where \( \alpha, \beta\in \mathbb{Z}[[\sqrt{-5}]] \). Then \( N(3)=9=N(\alpha)N(\beta) \). So we have two cases. If \( N(\alpha)=3 \) and \( \alpha=x+wy \) then we have \( x^2+5y^2=3 \) which is impossible. Similarly \( N(\beta)\neq 3 \). Therefore \( N(\alpha)=1 \) or \( N(\beta)=1 \) and hence \( 3 \) is irreducible. \( \Box \)

We have shown that irreducible numbers in \( \mathbb{Z}[[\sqrt{-5}]] \) need not to be prime. Next we will prove that in \( \mathbb{Z}[w] \) irreducible numbers are prime.

Lemma 2.4 If \( \alpha\in \mathbb{Z}[w] \) is irreducible, and \( \alpha \) does not divide \( a \) then \( \text{gcd}(a,\alpha)=1 \).
Proof. Let \( d \in \gcd(a, \alpha) \). Since \( \alpha \) is irreducible then 
\[ \alpha = dq \] where \( q \) or \( d \) is a unit. If \( q \) is a unit then \( d \) is an
associate of \( \alpha \), \( a = q'd = q'q^{-1} \alpha \) which results in a
contradiction since \( \alpha \) does not divide \( a \). So \( d \) is a unit
and \( \gcd(a, \alpha) = 1 \). □

Lemma 2.5 If \( \alpha, \beta \in \mathbb{Z}[w] \) are irreducible and \( \alpha \) is not an
associate of \( \beta \) then \( \gcd(\alpha, \beta) = 1 \).

Proof. If \( \alpha, \beta \) are irreducible and \( \alpha \) is not an
associate of \( \beta \) then \( \alpha \) does not divide \( \beta \). From the
preceding Lemma, we can say that \( \gcd(\alpha, \beta) = 1 \). □

Proposition 2.2 Let \( \alpha, a \) and \( b \in \mathbb{Z}[w] \). If \( \alpha \) is
irreducible and \( \alpha|ab \) then \( \alpha|a \) or \( \alpha|b \).

Proof. Assume \( \alpha|ab \) and \( \alpha \) does not divide \( a \). Therefore
\( \gcd(\alpha, a) = 1 \) and, by Lemma 2.3, we conclude \( 1 = s\alpha + ta \) for \( s, t \in \mathbb{Z}[w] \). If we multiply by \( b \) the equation becomes \( b = bs\alpha + tab \).
Now, \( ab = q\alpha \) for a certain \( q \in \mathbb{Z}[w] \) so \( b = bs\alpha + tq\alpha = (bs + tq)\alpha \).
Therefore \( \alpha|b \). □

Lemma 2.6 Let \( \lambda = 1-w \). Then \( \lambda^2 \) is an associate of \( \lambda \).

Further, if \( \alpha \in \mathbb{Z}[w] \) then \( \alpha \equiv -1, 0, \text{or } 1 \pmod{\lambda} \).

Proof. First, \( \lambda^2 = (1-w)^2 = 1 - 2w + w^2 = 1 - 2w - w - 1 = -3w \). Now
let \( \alpha = a + wb = a + (1-\lambda)b = a + b - \lambda b \). As a result, \( \alpha \equiv a + b \pmod{\lambda} \).
We have left to prove that \(a + b \equiv 0, 1, \text{or} -1 \pmod{\lambda}\). Let 
\[a + b = 3q + r\] where \(-1 \leq r \leq 1\) then \(a \equiv 3q + r \equiv r \pmod{\lambda}\). □

In Lemma 2.7 we will find the units in \(\mathbb{Z}[w]\).

Lemma 2.7 The units in \(\mathbb{Z}[w]\) are \(\{\pm 1, \pm w, \pm (1+w)\}\).

Proof. Assume that \(u = x + wy \in \mathbb{Z}[w]\) is a unit. Then there exist \(v \in \mathbb{Z}[w]\) such that \(uv = 1\). So \(N(u)N(v) = 1\). Then

\[x^2 - xy + y^2 = (x - y)^2 + xy = 1.\]

We have four cases. The first case when \(x > 0\) and \(y > 0\) then \(x = y = 1\) and \(u = 1 + w\). The second case when \(x < 0\) and \(y < 0\) then \(-x > 0\) and \(-y > 0\) so \(x = y = -1\) and \(u = -(1 + w)\). The third case when \(xy < 0\) and \(x^2 - xy + y^2 = 1\) is not possible. The last case when \(x = 0\) or \(y = 0\) then \(x^2 = 1\) or \(y^2 = 1\) so \(x = \pm 1\) or \(y = \pm 1\). Thus \(u = \pm 1\) or \(u = \pm w\).

We conclude that \(\mathbb{Z}[w]\) has six units \(\{1, -1, w, -w, w^2, -w^2\}\). □

The following two Propositions are used to find the prime numbers in \(\mathbb{Z}[w]\).

Proposition 2.3 If \(\pi\) is a prime in \(\mathbb{Z}[w]\) then there exist a rational prime \(p\) such that \(N(\pi) = p\) or \(p^2\). If \(N(\pi) = p\) then \(\pi\) is not an associate of a rational prime. If \(N(p) = p^2\) then \(\pi\) is an associate of \(p\).

Proof. Since \(N(\pi) = \pi \overline{\pi} > 0\), \(\pi \overline{\pi}\) is a product of rational primes \(p_1, p_2, \ldots p_k\). Therefore \(\pi | p_n\) for some \(p_n = p\) where \(p = \gamma \pi\).
and \( \gamma \in \mathbb{Z}[w] \). Now \( N(p) = N(\gamma)N(\pi) \) so \( p^2 = N(\gamma)N(\pi) \) and \( N(\pi) \neq 1 \).

Thus \( N(\pi) = p \) or \( p^2 \).

Proposition 2.4 If \( \pi \in \mathbb{Z}[w] \) and \( N(\pi) = p \) then \( \pi \) is a prime in \( \mathbb{Z}[w] \).

Proof. Assume that \( \pi = ab \) where \( a, b \in \mathbb{Z}[w] \) then
\( N(\pi) = N(a)N(b) = p \) so \( N(a) = 1 \) or \( N(b) = 1 \). We can conclude that \( a \) or \( b \) must be a unit. Thus \( \pi \) is irreducible. By Lemma 2.3, \( \pi \) is a prime.

Next we will find the primes in \( \mathbb{Z}[w] \).

Proposition 2.5 Let \( p \) be a rational prime. If \( p \equiv 2 \pmod{3} \) then \( p \) is a prime in \( \mathbb{Z}[w] \). If \( p \equiv 1 \pmod{3} \) then \( p = \pi \overline{\pi} \) where \( \pi \) is a prime in \( \mathbb{Z}[w] \). If \( p = 3 \) then \( 3 = -w^2(1-w) \) and \( (1-w) \) is a prime in \( \mathbb{Z}[w] \).

Proof. Suppose \( p \) is a rational prime but not a prime in \( \mathbb{Z}[w] \). Then \( p = \lambda \pi \) where \( N(\lambda) > 1 \) and \( N(\pi) > 1 \). Consider the case where \( N(\pi) = p \). Then \( p = a^2 - ab + b^2 \) where \( a, b \in \mathbb{Z} \). This implies \( 4p = 4a^2 - 4ab + b^2 + 3b^2 \) and \( 4p = (2a-b)^2 + 3b^2 \). Then \( p \equiv (2a-b)^2 \pmod{3} \). Now if \( x \in \mathbb{Z} \) and \( 3 \) does not divide \( x \) then \( x^2 \equiv 1 \pmod{3} \). Thus \( (2a-b)^2 \equiv 1 \pmod{3} \) since \( 3 \) does not divide \( 2a-b \). As a result, the congruence \( p \equiv 1 \pmod{3} \) is true. We have shown that if \( p \) is a rational prime and \( p \) is not a
prime in \( \mathbb{Z}[w] \) then \( p \equiv 1 \text{(mod 3)} \). Therefore if \( p \equiv 2 \text{(mod 3)} \) then \( p \) is a prime in \( \mathbb{Z}[w] \).

Assume now that \( p \equiv 1 \text{(mod 3)} \). Then by Theorem 1.1

\[
\left( \frac{-3}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{3}{p} \right) = \left( -1 \right)^{\frac{p-1}{2}} \left( \frac{3}{p} \right) \left( -1 \right)^{\frac{p-1}{2}} = \left( \frac{p}{3} \right).
\]

Since \( p \equiv 1 \text{(mod 3)} \) therefore

\[
\left( \frac{p}{3} \right) = \left( \frac{1}{3} \right) = 1.
\]

Since \( \left( \frac{-3}{p} \right) = 1 \) there exist \( a \in \mathbb{Z} \) such that

\[a^2 \equiv -3 \text{(mod } p\text{)}\.\] This implies that \( a^2 + 3 = pq \) where \( q \in \mathbb{Z} \). Now

\[a^2 + 3 = pq = (a - \sqrt{-3})(a + \sqrt{-3})\]. If \( p \) is a prime in \( \mathbb{Z}[w] \) then

\[p\mid (a - \sqrt{-3}) \text{ or } p\mid (a + \sqrt{-3})\]. Now \( 1 + 2w = \sqrt{-3} \) since \( w = -\frac{1}{2} + \frac{\sqrt{3}}{2} \) so

\[p\mid (a - 1 - 2w) \text{ or } p\mid (a + 1 + 2w)\]. If there exist \( \alpha, \beta \in \mathbb{Z} \) such that

\[p(\alpha + \beta w) = p\alpha + p\beta w = \alpha \pm 1 \pm 2w \text{ then } p\beta = \pm 2 \text{ which is a contradiction since } p \text{ is a prime in } \mathbb{Z} \text{ and } p \neq 2\]. Therefore \( p \) is not a prime in \( \mathbb{Z}[w] \).

Let \( p = \pi \gamma \) where \( \pi \) and \( \gamma \) are non-units. Then in \( \mathbb{Z}[w] \)

\[p^2 = N(\pi)N(\gamma) \text{ so } N(\pi) = N(\gamma) = p \text{ and } p = \pi \pi\].

Now \( x^3 - 1 = (x-1)(x-w)(x-w^2) \) implies \( x^2 + x + 1 = (x-w)(x-w^2) \). Let \( x = 1, \) \( 3 = (1-w)(1-w^2) = (1-w)^2(1+w) \) implies \( 3 = (1-w)^2(-w^2) \). By taking norms we get \( 9 = N[(1-w)^2] = N(1-w)N(1-w) \). Therefore \( N(1-w) = 3 \) which implies \( 1-w \) is prime by Proposition 2.4. \( \square \)
In conclusion, the prime elements of $\mathbb{Z}[w]$ are $\lambda=1-w$, the rational primes $p$ such that $p \equiv 2 \pmod{3}$, $r+ws$ and $r+w^2s$ when $p \equiv 1 \pmod{3}$ and $p = r^2 - rs + s^2$.

Example 2.2 Since $11 \equiv 2 \pmod{3}$, 11 is a prime in $\mathbb{Z}[w]$. Similarly $17 \equiv 2 \pmod{3}$ so 17 is a prime in $\mathbb{Z}[w]$. Now $7 \equiv 1 \pmod{3}$ then we can write $7 = (a+bw)(a+bw) = a^2 - ab + b^2$. Thus $a = 3$ and $b = 2$. So $7 = (3+2w)(3+2w^2)$. Therefore $3+2w$ and $3+2w^2$ are both prime in $\mathbb{Z}[w]$.

Proposition 2.6 Every element in $\mathbb{Z}[w]$ can be expressed uniquely as a product of irreducible numbers.

Proof. Let $S = \{a \in \mathbb{N} \text{ such that } a \text{ is not a product of irreducible numbers}\}$. Suppose $S$ is not empty. So by the Well-Ordering Principle $S$ must have an element $\alpha$ with minimum norm. Assume $\alpha \in S$ is the minimum. Then $\alpha$ is not an irreducible since otherwise $\alpha = \alpha$ is a representation of $\alpha$ as a product of irreducibles. Therefore $\alpha = \beta \gamma$ where $N(\beta) < N(\alpha)$ and $N(\gamma) < N(\alpha)$. Therefore $N(\beta) < N(\alpha)$ which implies $\beta \in S$. Therefore $\beta = \prod_{i=1}^{n} \beta_i$ and similarly $\gamma = \prod_{i=1}^{m} \gamma_i$. Therefore $\alpha = \beta \gamma = \prod_{i=1}^{n} \beta_i \prod_{i=1}^{m} \gamma_i$ which contradicts the definition of $\alpha$. Now for uniqueness, assume that $\alpha = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$ where $u$ and $u'$
are units, $p_i$ and $q_j$ are primes, and assume that $m>n$. One of the $p_i$ must divide $\prod_{j=1}^{m} q_j$. Since $p_m$ divides $\prod_{j=1}^{m} q_j$, there exist $i$ for which $p_m$ divides $q_i$. We may assume $i=m$. We cancel the common factor to get $\nu \prod_{i=1}^{m} p_i = \nu' \prod_{j=1}^{m} q_j$ where $\nu$, $\nu'$ are units. We will keep doing the same process until all the $p_i$'s are cancelled. Therefore, we will have $1=\prod_{n+1}^{m} q_j$ which is a contradiction. The proof is now complete. □
CHAPTER THREE

If \((x,y,z)\) is a Pythagorean triple and \(d\) is a common factor of \(x, y\) and \(z\), say \(x = dx', y = dy'\) and \(z = dz'\) then

\[(x')^2 + (y')^2 = (z')^2.\]

Definition 3.1 A Pythagorean triple is a set of three integers \((x, y, z)\) such that \(x^2 + y^2 = z^2\); the triple is said to be primitive if \(\gcd(x, y, z) = 1\).

The following Lemma is important in the proof of Fermat's Last Theorem for the case \(n=4\).

Lemma 3.1 If \((x, y, z)\) is a primitive Pythagorean triple then one of the integers \(x\) and \(y\) is even while the other is odd.

Proof. If \(x\) and \(y\) are both even, then \(2|2(x^2 + y^2)\) or \(2|z^2\), so that \(2|z\). The inference is that \(\gcd(x, y, z) \geq 2\), contradicting \(\gcd(x, y, z) = 1\). If, on the other hand, \(x\) and \(y\) are both odd, then \(x^2 \equiv 1 (mod 4)\) and \(y^2 \equiv 1 (mod 4)\), leading to \(z^2 = x^2 + y^2 \equiv 2 (mod 4)\). But this is impossible, since the square of any integer must be congruent to either 0 or 1 mod 4. In conclusion one of these integers \(x, y\) must be even and the other one is odd. \(\square\)

Note that \(z\) must be odd since either \(x\) or \(y\) must be even and the other one is odd.
The next Lemma shows that if a \( n \)th power is the product of two relatively prime factors then each factor must be a \( n \)th power.

Lemma 3.2 Let \( a, b, c \) be positive integers such that \( ab = c^n \), where \( \gcd(a, b) = 1 \), then \( a \) and \( b \) are \( n \)th powers; that is, there exist positive integers \( a_i, b_i \) for which \( a = a_i^n \), \( b = b_i^n \).

Proof. Assume that \( a > 1, b > 1 \). If \( a = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} \), \( b = q_1^{j_1} q_2^{j_2} \ldots q_s^{j_s} \) and \( c = u_1^{n_1} u_2^{n_2} \ldots u_t^{n_t} \) are the prime factorizations of \( a, b \) and \( c \). No \( p_i \) can occur among the \( q_i \), since \( \gcd(a, b) = 1 \).

As a result, the prime factorization of \( ab \) is given by \( ab = p_1^{k_1} \ldots p_r^{k_r} q_1^{j_1} \ldots q_s^{j_s} \), then \( ab = c^n \) becomes

\[
p_1^{k_1} \ldots p_r^{k_r} q_1^{j_1} \ldots q_s^{j_s} = u_1^{n_1} u_2^{n_2} \ldots u_t^{n_t}.
\]

From this, the primes \( u_1, \ldots, u_t \) are \( p_1, \ldots, p_r, q_1, \ldots, q_s \) in some order and \( n_1, \ldots, n_t \) are the corresponding exponents \( k_i, \ldots, k_r, j_1, \ldots, j_s \). The conclusion: each of the integers \( k_i \) and \( j_i \) must be divisible by \( n \). If we now put

\[
a_i = (p_1)^{k_i} (p_2)^{k_2} \ldots (p_r)^{k_r}, \quad b_i = (q_1)^{j_i} (q_2)^{j_2} \ldots (q_s)^{j_s},
\]

then \( a_i^n = a, \ b_i^n = b \), as desired. \( \Box \)

We will use the Pythagorean triples and the preceding Lemma to prove the following Theorem, which is necessary for the proof of Fermat's Last Theorem in the case \( n = 4 \).
Theorem 3.1 All solutions of the Pythagorean equation \( x^2 + y^2 = z^2 \) satisfying the conditions \( \gcd(x, y, z) = 1, 2 | x, \)
\( x > 0, y > 0, z > 0 \) are given by the formulas \( x = 2st, \quad y = s^2 - t^2, \)
\( z = s^2 + t^2 \) for integers \( s > t > 0 \) such that \( \gcd(s, t) = 1 \) and \( s \not\equiv t \pmod{2} \).

Proof. Let \( x, y, z \) be a positive primitive Pythagorean triple. Let \( x \) even, \( y \) and \( z \) both odd. Then \( z - y \) and \( z + y \) are even integers, \( z - y = 2u \) and \( z + y = 2v \). Now the equation \( x^2 + y^2 = z^2 \) may be rewritten as \( x^2 = z^2 - y^2 = (z - y)(z + y) \). Whence
\[
\frac{x}{2} = \frac{(z - y)(z + y)}{2} = uv \quad \text{where} \quad u = \frac{z - y}{2}, \quad v = \frac{z + y}{2}.
\]
If \( \gcd(u, v) = d \) then \( d | (u - v) \) and \( d | (u + v) \), or \( d | y \) and \( d | z \). Since \( \gcd(y, z) = 1 \), \( d = 1 \). By taking Lemma 3.2 into consideration, we may conclude that \( u \) and \( v \) are each perfect square. Let \( u = t^2, v = s^2 \) where \( s \) and \( t \) are positive integers. Now
\[
z = u + v = s^2 + t^2,
\]
\[
y = v - u = s^2 - t^2,
\]
\[
x^2 = 4uv = 4s^2t^2.
\]

It follows that \( x = 2st \). Since any common factor of \( s \) and \( t \) would divide both \( y \) and \( z \), the condition \( \gcd(y, z) = 1 \) forces \( \gcd(s, t) = 1 \). It remains to prove that \( s \not\equiv t \pmod{2} \). The preceding statement means that one is even and the other is odd. Assume the contrary that both \( s \) and \( t \) are both even or
both odd, then \( y = s^2 - t^2 \) and \( z = s^2 + t^2 \) would be even which is impossible since \( \gcd(y, z) = 1 \). Assume, without lost of generality, that \( s \) is even and \( t \) is odd then \( s \equiv t (\text{mod} 2) \). □

Example 3.1 Pythagorean Triples: We can generate all Pythagorean Triples by using the parameters \( s \) and \( t \). For \( s = 2 \) and \( t = 1 \) we have \( x = 4, \ y = 4 - 1 = 3 \) and \( z = 4 + 1 = 5 \). Now for \( s = 4, \ t = 3 \) or \( t = 1 \). For \( s = 4 \) and \( t = 3 \), we have \( x = 24, \ y = 7 \) and \( z = 25 \). For \( s = 4 \) and \( t = 1 \), we have \( x = 8, \ y = 15 \) and \( z = 17 \). For \( s = 6, \ t = 5, 3 \) or \( t = 1 \). If \( s = 6 \) and \( t = 5 \) then \( x = 60, \ y = 11 \) and \( z = 61 \). If \( s = 6 \) and \( t = 3 \) then \( x = 36, \ y = 27 \) and \( z = 45 \). Finally, if \( s = 6 \) and \( t = 1 \) then \( x = 12, \ y = 35 \) and \( z = 37 \). Similarly we are able to generate all Pythagorean Triples.

Now we can deal with the proof of Fermat's Last Theorem in the case \( n = 4 \). We will accomplish our goal by proving a more general result: \( x^4 + y^4 = z^2 \) has no solution in positive integers \( x, y \) and \( z \).

Theorem 3.2 The equation \( x^4 + y^4 = z^2 \) has no solution in positive integers \( x, y \) and \( z \).

Proof. Assume that there exists a positive solution \( x_0, y_0, z_0 \) of \( x^4 + y^4 = z^2 \). We may also assume that \( \gcd(x_0, y_0) = 1 \). Otherwise, let \( \gcd(x_0, y_0) = d, x_0 = dx_1, y_0 = dy_1, z_0 = d^2 z_1 \) to get instead \( x_1^4 + y_1^4 = z_0^2 \) with \( \gcd(x_1, y_1) = 1 \).
By expressing the equation \( x_0^4 + y_0^4 = z_0^2 \) in the form
\[
(x_0^2)^2 + (y_0^2)^2 = z_0^2,
\]
We can see that \( x_0^2, y_0^2, z_0 \) meet all the requirements of a primitive Pythagorean triple, so there exist \( s > t > 0 \) satisfying
\[
\begin{align*}
x_0^2 &= 2st, \\
y_0^2 &= s^2 - t^2, \\
z_0 &= s^2 + t^2,
\end{align*}
\]
(Assume that \( x_0 \) is even), where exactly one of \( s \) and \( t \) is even. Assume that \( s \) is odd so \( t = 2r \) for a certain \( r \). Then the equation \( x_0^2 = 2st \) becomes \( x_0^2 = 4sr \) and \( (x_0/2)^2 = rs \), (Note that \( \gcd(s, t) = 1 \) implies that \( \gcd(s, r) = 1 \)). We can conclude that the product of two relatively prime integers is a square; hence, by Lemma 3.2 \( s = z_i^2, r = w_i^2 \) for positive integers \( z_i, w_i \).

Since \( y_0^2 = s^2 - t^2 \) then \( t^2 + y_0^2 = s^2 \) and since \( \gcd(s, t) = 1 \), it follows that \( \gcd(t, y_0, s) = 1 \), making \( t, y_0, s \) a primitive Pythagorean triple. With \( t \) even, we obtain
\[
\begin{align*}
t &= 2uv, \\
y_0 &= u^2 - v^2, \\
s &= u^2 + v^2,
\end{align*}
\]
for relatively prime integers \( u > v > 0 \). Now the relation
\[
 uv = \frac{t}{2} = r = w_i^2
\]
means that \( u \) and \( v \) are both squares, say \( u = x_i^2 \).
and \( v = y_1^2 \). When these values are substituted into the equation for \( s \), the result is
\[
z_i^2 = s = u^2 + v^2 = x_i^4 + y_i^4.
\]

We also have the inequality
\[
0 < z_i \leq z_i^2 = s < s^2 + t^2 = z_0.
\]

Now, we have constructed another solution \( x_i, y_i, z_i \) such that \( 0 < z_i < z_0 \). Repeating the whole argument, we will find another solution such that \( 0 < z_2 < z_1 < z_0 \). This process can be carried out as many times to produce an infinite decreasing sequence of positive integers
\[
z_0 > z_1 > z_2 > \ldots.
\]

Since there is only a finite supply of positive integers less than \( z_0 \), a contradiction occurs.

We conclude that \( x^4 + y^4 = z^2 \) is not solvable in the positive integers. \( \square \)

Fermat proved his conjecture for the case \( n=4 \) around 1630. It was over hundred years before a proof was given for the case \( n=3 \). One obstacle seems to be the need to understand arithmetic for complex numbers. The complex number \( \lambda = 1 - w \) plays an important role in the infinite descent portion of the proof.
Definition 3.2 If $a \in \mathbb{Z}[\omega]$ and $a = u\lambda^\nu b$ where $u$ is a unit in $\mathbb{Z}[\omega]$, $\lambda = 1 - \omega$ and $\lambda$ does not divide $b$ then we define $\text{ord}(a) = n$.

Note that $\lambda$ is a prime in $\mathbb{Z}[\omega]$ by Proposition 2.5.

Lemma 3.3 Let $x, y \in \mathbb{Z}[\omega]$ then $\text{ord}(xy) = \text{ord}(x)\text{ord}(y)$.

Proof. Let $x = u\lambda^{\text{ord}(x)} b$ where $u$ is a unit of $x$ and $\lambda$ does not divide $b$ and $y = v\lambda^{\text{ord}(y)} c$ where $v$ is a unit of $y$ and $\lambda$ does not divide $c$. Then $xy = uv\lambda^{\text{ord}(x)+\text{ord}(y)} bc = w\lambda^d$ where $\lambda$ does not divide $bc$ because if $\lambda | bc$ then $\lambda | b$ or $\lambda | c$ which is impossible. We can now conclude that $\text{ord}(xy) = \text{ord}(x) + \text{ord}(y)$. □

Lemma 3.4 Let $a, b \in \mathbb{Z}[\omega]$ such that $\text{ord}(a) \neq \text{ord}(b)$ then $\text{ord}(a+b) = \min\{\text{ord}(a), \text{ord}(b)\}$.

Proof. Let $a, b \in \mathbb{Z}[\omega]$ such that $a = u\lambda^{\text{ord}(a)} c$ where $u$ is a unit and $\lambda$ does not divide $c$ and $b = v\lambda^{\text{ord}(b)} d$ where $v$ is a unit and $\lambda$ does not divide $d$. Assume $\text{ord}(a) \leq \text{ord}(b)$, then $a + b = w\lambda^{\text{ord}(a+b)} m = \lambda^{\text{ord}(a)} [uc + \lambda^{\text{ord}(b) - \text{ord}(a)} vd]$. We know that $\lambda$ does not divide $uc + \lambda^{\text{ord}(b) - \text{ord}(a)} vd$ and $\lambda^{\text{ord}(a)} | (a+b)$. We can now conclude that $\text{ord}(a+b) = \text{ord}(a)$. Therefore $\text{ord}(a+b) = \min\{\text{ord}(a), \text{ord}(b)\}$. □

The following Lemma is an important result used in the proof of Fermat’s Last Theorem when $n=3$.  

30
Lemma 3.5 Let $Z$ be an ideal of $\mathbb{Z}$, and let $n \equiv 1 \pmod{\mathbb{Z}}$. Then $n \equiv 1 \pmod{\mathbb{Z}}$.

Proof. We know that if $n \equiv 1 \pmod{\mathbb{Z}}$ then $n \equiv 1 \pmod{\mathbb{Z}}$. Then $n \equiv 1 \pmod{\mathbb{Z}}$. Since $n \equiv 1 \pmod{\mathbb{Z}}$ and by Lemma 3.5.

Lemma 3.6 Let $\alpha$ be a unit in $\mathbb{Z}$. Let $x, y \in \mathbb{Z}$ such that $x + y = \alpha$. If $\alpha$ does not divide $xy$ and $x + y = \alpha$, then $x = \pm 1 \pmod{\mathbb{Z}}$ and $y = \pm 1 \pmod{\mathbb{Z}}$. Therefore, $\alpha$ is a unit in $\mathbb{Z}$.

Proof. If $x = 1 \pmod{\mathbb{Z}}$, then by Lemma 3.5, $x = 1 \pmod{\mathbb{Z}}$. Also if $x = -1 \pmod{\mathbb{Z}}$ then $x = 1 \pmod{\mathbb{Z}}$. So $x = \pm 1 \pmod{\mathbb{Z}}$. Therefore, $\alpha$ is a unit in $\mathbb{Z}$.

Now suppose that $\alpha$ is a unit in $\mathbb{Z}$. Since $\alpha$ is a unit in $\mathbb{Z}$, we know that $\alpha$ is not a unit in $\mathbb{Z}$. Therefore, $\alpha$ is not a unit in $\mathbb{Z}$. Therefore, $\alpha$ is a unit in $\mathbb{Z}$.

For $\alpha = 1 \pmod{\mathbb{Z}}$, then by Lemma 3.5, $\alpha = 1 \pmod{\mathbb{Z}}$. Therefore, $\alpha$ is a unit in $\mathbb{Z}$.
sides \( N(2) = N(\alpha \lambda) = N(\alpha)N(\lambda), \) \( 4 = N(\alpha)3 \) which is impossible since \( N(2) = 4 \) and \( N(\lambda) = 3 \). Thus \( \lambda \) does not divide 2. Hence \( \varepsilon z^3 \equiv \pm 2 (\text{mod} \lambda^4) \) is not possible. The only case left is when \( \varepsilon z^3 \equiv 0 (\text{mod} \lambda^4) \) giving \( 3 \text{ord}(z) \geq 4 \text{ord}(\lambda) \) or \( \text{ord}(z) \geq \frac{4}{3} \). So we can conclude that \( \text{ord}(z) \geq 2 \). □

The proof of the next Lemma is identical to that of Lemma 2.2

Lemma 3.7 Let \( a, b, c \in \mathbb{Z}[w] \) with \( \gcd(a, b) = 1 \). If \( ab = c^n \) there exist positive integer \( n \) such that \( a = \alpha^n, \ b = \beta^n \) for \( \alpha, \beta \in \mathbb{Z}[w] \).

In the following Lemma, we will demonstrate the idea of decreasing the order of one of the variables by one in the case \( n = 3 \) of Fermat's Last Theorem.

Lemma 3.8 Suppose \( x^3 + y^3 = \varepsilon z^3 \) where \( \varepsilon \) is a unit in \( \mathbb{Z}[w] \), \( \gcd(x, y) = 1 \), \( \lambda \) does not divide \( xy \) and \( \text{ord}(z) \geq 2 \). Then we can find \( x', y', z' \) and a unit \( \varepsilon' \) in \( \mathbb{Z}[w] \) to satisfy \( x'^3 + y'^3 = \varepsilon' z'^3 \), \( \lambda \) does not divide \( x'y' \), and \( \text{ord}(z') = \text{ord}(z) - 1 \).

Proof. The following equality \( x^3 + y^3 = \varepsilon z^3 \) can be factored as \( (x + y)(x + wy)(x + w^2y) = \varepsilon z^3 \). Now, since \( \text{ord}(z) \geq 2 \), then \( \text{ord}(z^3) = 3 \text{ord}(z) \geq 6 \) and we can conclude that \( \text{ord}(\varepsilon z^3) \geq 6 \). Consider now the following equation \( (x + y)(x + wy)(x + w^2y) = \varepsilon z^3 \).
since $\lambda^6$ divide $\varepsilon z^3$, one of the factors on the left hand side must be divisible by $\lambda^2$. Assume without lost of generality that $\text{ord}(x+y) \geq 2$. Now $\text{ord}(\lambda y) = 1$ so $\text{ord}(\lambda y) \neq \text{ord}(x+y)$. Therefore from Lemma 3.4 we conclude:

$$\text{ord}(x+wy) = \text{ord}(x+y-(1-w)y)$$

$$= \text{ord}(x+y-\lambda y)$$

$$= \min(\text{ord}(x+y), \text{ord}(\lambda y))$$

$$= \min(2,1) = 1.$$ 

Using a similar argument we also have $\text{ord}(x+w^2y) = 1$.

Therefore,

$$\text{ord}[(x+y)(x+wy)(x+w^2y)] = \text{ord}[\varepsilon z^3]$$

$$\text{ord}(x+y) + \text{ord}(x+wy) + \text{ord}(x+w^2y) = \text{ord}[\varepsilon z^3]$$

$$\text{ord}(x+y) + 1 + 1 = 3\text{ord}(z)$$

$$\text{ord}(x+y) = 3\text{ord}(z) - 2.$$ 

We show next that $\lambda \notin \text{gcd}(x+y, x+wy)$. We can rewrite our equality in the following form

$$\frac{x+y}{\lambda^{\text{ord}(\varepsilon)}} \times \frac{x+wy}{\lambda} \times \frac{x+w^2y}{\lambda} = \varepsilon \left( \frac{z}{\lambda^{\text{ord}(\varepsilon)}} \right)^3$$

with the factors on the left hand side relatively prime. If $\phi$ is an irreducible element not an associate of $\lambda$ such that $\phi(x+y)$ and $\phi(x+wy)$ then $\phi(1-w)y$. Since $\phi$ is not an associate of $\lambda$, $\phi\mid y$. Similarly $\phi\mid x$ contrary to the assumption that $\text{gcd}(x,y) = 1$. Similar arguments show that
\[\lambda \in \gcd(x + y, x + w^2 y)\) and \(\lambda \in \gcd(x + wy, x + w^2 y)\). Thus, by Lemma 3.7, we have the following:
\[x + y = \varepsilon_1 \alpha^3 \lambda^{3 \operatorname{ord}(z)^{-2}}\]
\[x + wy = \varepsilon_2 \beta^3 \lambda\]
\[x + w^2 y = \varepsilon_3 \gamma^3 \lambda,\]
where \(\lambda\) does not divide \(\alpha, \beta,\) or \(\gamma,\)
\[\gcd(\alpha, \beta) = \gcd(\beta, \gamma) = \gcd(\gamma, \alpha) = 1,\] and \(\varepsilon_1, \varepsilon_2,\) and \(\varepsilon_3\) are units.
Since \(1 + w + w^2 = 0\), we conclude that
\[\varepsilon_1 \alpha^3 \lambda^{3 \operatorname{ord}(z)^{-2}} + w \varepsilon_2 \beta^3 \lambda + w^2 \varepsilon_3 \gamma^3 \lambda = 0.\]
Divide now by \(\lambda w\varepsilon_2\) to get
\[\beta^3 + \varepsilon_4 \gamma^3 = \varepsilon_5 \alpha^3 \lambda^{3 \operatorname{ord}(z)^{-1}},\]
where \(\varepsilon_4 = w \varepsilon_2^{-1} \varepsilon_3\) and \(\varepsilon_5 = -w^{-1} \varepsilon_2^{-1} \varepsilon_1\) are both units. Now since \(\theta \in \mathbb{Z}[w]\) implies \(\theta \equiv -1, 0, 1, (\mod \lambda)\) and \(\theta \equiv 1 (\mod \lambda)\) implies \(\theta^3 \equiv 1 (\mod \lambda^3)\), (Lemma 3.5), we will have, as \(\lambda\) does not divide \(\alpha, \beta,\) or \(\gamma,\)
\[\pm 1 \pm \varepsilon_4 \equiv 0 (\mod \lambda^2).\]
Now since, \(\pm \alpha \equiv 1 (\mod \lambda)\) implies \(\alpha^3 \equiv \pm 1 (\mod \lambda^3)\) and \(\lambda^2\) is an associate of \(3\) then \(\varepsilon_4 = \pm 1.\) Let \(x' = \beta\) and \(y' = \pm \gamma,\) where the sign depends on the sign of \(\varepsilon_4,\) and \(z' = \alpha \lambda^{\operatorname{ord}(z)-1}.\)

The following is the proof of Fermat's last theorem when \(n = 3.\)
Theorem 3.3 Let $\varepsilon$ be a unit in $\mathbb{Z}[w]$. The equation
$x^3 + y^3 = \varepsilon z^3$ has no solution $\{x, y, z\}$ where $x, y, z \in \mathbb{Z}[w]$ and
$x, y, z \neq 0$.

Proof. We break the proof into four cases.

Case 1. Assume that $x^3 + y^3 = \varepsilon z^3$ has a solution $\{x, y, z\}$
where $\lambda$ does not divide $x, y, z$. Since $\lambda$ does not divide $x$,
$x \equiv \pm 1 \pmod{\lambda}$. Similarly $y, z \equiv \pm 1 \pmod{\lambda}$. Therefore
$\pm 1 \pm 1 \equiv \varepsilon_4 \pmod{\lambda^4}$ which is impossible as 9 is an associate of
$\lambda^4$ and $\varepsilon_4$ is a unit and the units in $\mathbb{Z}[w]$ are $\pm 1, \pm w, \pm (1+w)$.

Case 2. Assume that $x^3 + y^3 = \varepsilon z^3$ has a solution $\{x, y, z\}$
where $\lambda$ does not divide $x, y, z$. In this case we can
apply Lemma 3.6 and Lemma 3.8 to obtain a new solution
$\{x, y, z\}$ with $\text{ord}(z) < \text{ord}(z_2)$ and $\lambda$ does not divide $x, y, z$. We
will repeat the preceding until we will satisfy the
condition of case 1.

Case 3. Assume that $x^3 + y^3 = \varepsilon z^3$ has a solution $\{x, y, z\}$
with $\lambda | x$ and $\lambda$ does not divide $y, z$. In this case, Lemma
3.6 implies $\varepsilon \equiv \pm 1 \pmod{\lambda^4}$ and so $\varepsilon \equiv \pm 1$ since $\varepsilon$ is a unit.
Hence the equation can be rewritten as $(\pm z^3)^3 + (-y^3)^3 = x^3$ and
Case 2 now applies.
Case 4. Assume that \( x^3 + y^3 = \varepsilon z^3 \) has a solution \( \{x_5, y_5, z_5\} \) with \( \lambda | y_5 \) and \( \lambda \) does not divide \( x_5z_5 \). This is similar to case 3. □

Next we will prove an important result used to prove Sophie Germain’s theorem.

Lemma 3.9 If \( p \) is a prime and \( \gcd(a, p) = 1 \) then

\[
\frac{p-1}{a^2} \equiv \pm 1 \pmod{p}.
\]

Proof. Consider the numbers \( ax \), where \( x = 1, 2, ..., (p-1) \) are congruent in some order to the numbers \( 1, 2, ..., (p-1) \) therefore

\[ a2a3a...(p-1)a \equiv (123...(p-1))(\mod{p}) \]

and the following congruence is true \( a^{p-1}(p-1) \equiv (p-1)! \equiv (p-1)! \pmod{p} \). Now by Wilson’s Theorem

\( (p-1)! \equiv -1 \pmod{p}, \) \( a^{p-1} \equiv 1 \pmod{p} \) or \( a^{p-1} - 1 \equiv 0 \pmod{p} \) and by

factoring \( a^{p-1} - 1 \) we will get \( \frac{p-1}{a^2} - 1 + \frac{p-1}{a^2} \equiv 0 \pmod{p} \) then

\[
\frac{p-1}{a^2} \equiv \pm 1 \pmod{p}.
\]

□

The following Theorem is named after the French mathematician Sophie Germain.

Sophie Germain’s Theorem: Let \( p \) be an odd prime and \( q = 2p + 1 \) is also a prime then \( x^p + y^p + z^p = 0 \) has no solution in integers with \( xyz \neq 0 \) where \( p \) does not divide \( xyz \).

Proof. Assume \( x^p + y^p + z^p = 0 \) has a solution \( \{x_1, y_1, z_1\} \) with \( \gcd(x_1, y_1, z_1) = 1 \) and \( p \) does not divide \( x_1y_1z_1 \). Then
\( x_i^p + y_i^p + z_i^p = 0 \) and \( (-x_i)^p = y_i^p + z_i^p \). By factoring the preceding equation we get \( (-x_i)^p = (y_i + z_i)(y_i^p - y_i^{p-2}z_i + y_i^{p-3}z_i^2 - \ldots + z_i^{p-1}) \). Next we show that \( y_i + z_i \) and \( y_i^{p-1} - y_i^{p-2}z_i + y_i^{p-3}z_i^2 - \ldots + z_i^{p-1} \) are relatively prime. If \( \psi \) were a prime which divided them both then \( (y_i + z_i) \equiv 0 \pmod{\psi} \) so that \( y_i \equiv -z_i \pmod{\psi} \) and

\[
(y_i^{p-1} - y_i^{p-2}z_i + y_i^{p-3}z_i^2 - \ldots + z_i^{p-1}) \equiv 0 \pmod{\psi} \quad \text{and} \quad py_i^{p-1} \equiv 0 \pmod{\psi}.
\]

Now we have two cases. If \( p \equiv 0 \pmod{\psi} \) and since \( p \) is a prime number, \( p = \psi \) which results in a contradiction since \( p \) would divide \( x_i \). Now if \( y_i \equiv 0 \pmod{\psi} \) then \( \psi \mid y_i \) and \( \psi \mid (y_i + z_i) \) which is impossible. We conclude that \( (y_i + z_i) \) and

\[
(y_i^{p-1} - y_i^{p-2}z_i + y_i^{p-3}z_i^2 - \ldots + z_i^{p-1}) \]

are relatively prime. Now \( y_i + z_i = a^p \) and \( y_i^{p-1} - y_i^{p-2}z_i + y_i^{p-3}z_i^2 - \ldots + z_i^{p-1} = t^p \). Similarly,

\[
x_i + z_i = a^p \quad \text{and} \quad z_i^{p-1} - z_i^{p-2}x_i + z_i^{p-3}x_i^2 - \ldots + x_i^{p-1} = \alpha^p \quad \text{and} \quad x_i + y_i = b^p \quad \text{and}
\]

\[
x_i^{p-1} - x_i^{p-2}y_i + x_i^{p-3}y_i^2 - \ldots + y_i^{p-1} = \beta^p \quad \text{We can also rewrite} \quad -x_i^p = a^p \alpha^p.
\]

Thus \( -x_i = a^p \alpha^p \) implies that \( -x_i = at \). Similarly \( -y_i = c \alpha \) and \( -z_i = b \beta \).

We now show that \( q \mid x_i, y_i, z_i \). Suppose that \( q \) does not divide \( x_i, y_i, z_i \). By Lemma 3.9, \( x_i^p \equiv \pm 1 \pmod{q} \), \( y_i^p \equiv \pm 1 \pmod{q} \) and
\(z_i^p \equiv \pm 1 (\text{mod} q)\). Now since \(x_i^p + y_i^p + z_i^p \equiv 0 (\text{mod} q)\) then
\[\pm 1 \pm 1 \pm 1 \equiv 0 (\text{mod} q)\] which is impossible. Therefore \(q \mid x_i y_i z_i\).

Now assume that \(q \mid x_i\) and \(q\) does not divide \(y_i z_i\).

\[x_i + y_i = b^p \text{ implies } y_i \equiv b^p (\text{mod} q)\]
\[x_i + z_i = c^p \text{ implies } z_i \equiv c^p (\text{mod} q)\]
\[y_i + z_i = a^p \text{ implies } y_i + z_i \equiv a^p (\text{mod} q)\].

Then \(b^p + c^p \equiv a^p (\text{mod} q)\) and \(p = \frac{q - 1}{2}\) then

\[\frac{q - 1}{2} \frac{q - 1}{2} \frac{q - 1}{2} (\text{mod} q)\]. We are now able to conclude that

\[\frac{q - 1}{2} \frac{q - 1}{2} \frac{q - 1}{2} (\text{mod} q)\] which is a contradiction. \(\Box\)
CHAPTER FOUR

In Chapter Four, we first summarize the previous work in proving Fermat's Last Theorem for the case $n=3$ and $n=4$. Next, we discuss Sophie Germain's Theorem and some other cases like $n=5, 7$ and $n=14$. We will also mention some recent results including the proof of Fermat's Last Theorem.

Fermat wrote the statement of his Theorem around 1630, when he was studying Diophantus Arithmetica. Fermat wrote "I have discovered a truly remarkable proof which this margin is too small to contain". Fermat's only known proof was the case when $n=4$. Later Euler wrote to Goldbach on 4 August 1753 claiming he had the proof of Fermat's Theorem when $n=3$. Euler showed that if positive whole numbers $x, y, z$ could be found for which $x^3 + y^3 = z^3$ then smaller positive whole numbers could be found with the same property (method of infinite descent). However his proof needed to find cubes of the form $p^2 + 3q^2$. Euler also showed the converse that for any $a, b$ if we put $p = a^3 - 9ab, q = 3(a^2b - b^3)$ then $p^2 + 3q^2 = (a^2 + 3b^2)^3$. Euler showed that if $p^2 + 3q^2$ is a cube then $a$ and $b$ exist such that $p$ and $q$ are as above. The next major step forward was due to Sophie Germain. A special case of Sophie Germain's Theorem says that if the integers $n$ and $2n+1$ are primes then $x^n + y^n = z^n$ implies that one of $x, y, z$ is divisible by $n$. Hence Fermat's Last Theorem splits into two
cases. Case one where none of \(x, y, z\) is divisible by \(n\). Case two where one and only one of \(x, y, z\) is divisible by \(n\). For example, in the case \(n=7\) it is not true that \(2n+1=15\) is a prime but it is true that \(4n+1=29\) is prime. The \(7^{th}\) powers of all numbers less than \(29 \mod 29\) are \(0, \pm 1, \pm 12\) therefore \(x^7 + y^7 + z^7 \equiv 0\mod 29\) is possible only if one of the numbers is zero \(\mod 29\). Sophie Germain proved case one, where none of \(x, y, z\) is divisible by \(n\), of Fermat’s Last Theorem for all \(n\) less than 100 and Legendre extended her methods to all numbers less than 197. Now case two, where only one of \(x, y, z\) is divisible by \(n\), for \(n=5\) splits into two cases also. Case 2(i), was when the number divisible by 5 is even, which was proved by Dirichlet and presented to the Paris Academy in July 1825. Case 2(ii), was when the even number and the one divisible by 5 are distinct, which was proved by Legendre and published in September 1825. In 1832 Dirichlet published a proof of Fermat’s Last Theorem for \(n=14\). His proof depended on a technique which is essentially the same as the proof for \(n=5\). The proof depended also on a lemma which states that if \(a^2 + 7b^2\) is a \(14^{th}\) power and if \(7|b\) then

\[a + b\sqrt{-7} = (c + d\sqrt{-7})^{14}\]

for some integers \(c\) and \(d\). The \(n=7\) case was finally solved by Lame in 1839. On March first 1847 Lame announced to the Paris academy that he had proven Fermat’s Last Theorem using complex numbers. However Liouville
addressed the meeting after Lame and suggested that the uniqueness of factorization into primes was needed for these complex numbers. Cauchy supported Lame. Cauchy had an idea about the proof of Fermat's Last Theorem in the October meeting of 1847. Kummer's approach was to express the following $x^p + y^p$ as product of factors which are relatively prime and therefore must themselves be $p$th powers, since integers factored uniquely into primes. As a result

$$x^p + y^p = (x+y)(x+\zeta y)(x+\zeta^2 y) \cdots (x+\zeta^{p-1} y)$$

where $\zeta_p$ represents a $p$th root of unity. The various factors $x+y$, $x+\zeta y$, ..., $x+\zeta^{p-1} y$ are relatively prime. Kummer proved that, for every prime $p$, $p=\lambda (\text{mod} \lambda)$, where the prime $\lambda$ is the norm of some cyclotomic integer. The smallest prime for which $\mathbb{Q}[\zeta_p]$ does not satisfy the unique factorization property is $p=23$. In particular, it is a straightforward calculation to verify that

$$\left(1 + \zeta_2^2 + \zeta_2^4 + \zeta_2^5 + \zeta_2^6 + \zeta_2^{10} + \zeta_2^{11}\right) \left(1 + \zeta_2^1 + \zeta_2^5 + \zeta_2^6 + \zeta_2^7 + \zeta_2^9 + \zeta_2^{11}\right) = 2\zeta_2^{12}(1 + \zeta_2^1 + \zeta_2^2 + \zeta_2^4 + \zeta_2^5 + 3\zeta_2^6 + \zeta_2^7 + \zeta_2^8 + \zeta_2^{10} + \zeta_2^{11} + \zeta_2^{12}).$$

By September 1847 Kummer sent to Dirichlet and the Berlin Academy a paper proving that a prime $p$ is regular if $p$ does not divide the numerators of any Bernoulli numbers $b_2, b_4, \ldots, b_{p-3}$, where the Bernoulli number $b_n$ is defined by

$$\frac{x}{(e^x-1)} = \sum \frac{b_n}{n!}.$$
regular but 37 are not regular as 37 divide the numerator of $b_3$. The only primes less than 100 which are not regular are 37, 59 and 67.

More recent results related to Fermat’s Last Theorem were discovered by Wagstaff who proved in 1976 that Fermat’s Last Theorem holds for every prime exponent $p<125000$ and Morishima and Gunderson who, in 1948, proved that the first case of Fermat’s Last Theorem holds for every prime exponent $p<57 \times 10^9$. Terjanian in 1977 proved that if $x, y, z$ are nonzero integers, $p$ is an odd prime, and $x^{2p} + y^{2p} = z^{2p}$ then $2p$ divides $x$ or $y$.

In 1955 Yutaka Taniyama did some research about elliptic curves, curves of the form $y^2 = x^3 + ax + b$. Further work by Weil and Shimura produced a conjecture, now known as Shimura-Taniyama conjecture. The conjecture states that all elliptic curves are modular. The proof of Fermat’s Last Theorem was completed in 1993 by Andrew Wiles, a British mathematician working at Princeton in the USA. On Wednesday 23 June 1993 Wiles announced that he had a proof of Fermat’s Last Theorem as a corollary to his main results. Wiles had proved the Shimura-Taniyama conjecture for a class of examples. Some of those examples were sufficient to prove Fermat’s Last Theorem. This, however, is not the end of the story. On 4 December 1993 Wiles made a statement about a
number of problems that emerged in his proof. On October 6, 1994 Wiles sent a proof to three colleagues including Faltings. All liked the new proof, which was simpler than the earlier one.

The correctness of a proof this complex can be easily guaranteed, so a very small doubt will remain for some time. However when Taylor lectured at the British Mathematical Colloquium in Edinburg in April 1995 he gave the impression that no real doubts remained over the proof of Fermat’s Last Theorem. Today it is generally accepted that Wile’s proof is valid and that the proof of Fermat’s Last Theorem has finally been achieved.
REFERENCES


